UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

DIVISION OF
ENFORCEMENT

May 31, 2024

VIA ECF
Hon. Paul A. Engelmayer
United States District Court
Southern District of New York
40 Foley Square
New York, NY 10007

Re: ***SEC v. SolarWinds Corp. et al.*, No. 23-cv-09518-PAE**

Dear Judge Engelmayer:

Plaintiff, the United States Securities and Exchange Commission ("SEC"), respectfully submits this response to the recent letter filed by Defendants, SolarWinds Corp. ("SolarWinds") and Timothy Brown (ECF No. 123). The SEC addresses three issues herein, but does not again respond to Defendants' re-hashing of arguments regarding the motion to dismiss. First, the factual record in this case supports describing the attack on Palo Alto Networks ("Palo Alto") as an attack. Second, one of the SEC's theories in this case has consistently been that the ***similarity*** between the Palo Alto attack and the prior attack on the U.S. Trustee Program ("USTP") was a critical issue requiring disclosure. Third, these issues remain factual disputes.

First, although it does appear that the first discussion of the involvement of a red team was on November 5, SolarWinds and Palo Alto continued to describe the incident in terms of an attack after that point. *See* ECF No. 122-3 at 8 (SolarWinds continuing to use the term "***attack*** chain" on November 6); *id.* at 9 (SolarWinds employee on November 11: "they could have ***exploited*** that probably"); *id.* at 10 (SolarWinds employee relaying Palo Alto comment on November 12: "our theory is that SW was ***exploited*** sometime around 9/28 to stage the subsequent malware download a week later on 10/5"); *id.* at 13 (SolarWinds employee on November 26 noting that Palo Alto "thinks we're looking at an unknown vulnerability at play" and "suggests that we handle this as though it's an ***external attacker***.") (all emphasis added). Additionally, as the attack was not described as a red team exercise until November 5, Brown cannot rely on the red team excuse for his failure to elevate the linked attacks to the disclosure committee prior to that time.

Second, Defendants incorrectly claim that the SEC is trying to change theories. Not so. The SEC's theory has consistently remained that the attack on USTP and the attack on Palo Alto were part of a series of red flags[1] that collectively required SolarWinds to update their risk disclosures to note the increased risk that the company faced. Among the reasons for this was that Brown had described the attack on USTP as "unique" in part due to "additional software that

[1] *See* AC ¶¶ 261-266, 290-297 for additional red flags beyond the USTP and Palo Alto attacks.

was installed on the machine that was targeting SolarWinds." AC ¶ 275. Brown theorized at the time that there were two possibilities, either attackers had been present on USTP's systems before Orion was installed or attackers were looking to utilize Orion in a larger attack campaign. *See* AC ¶ 272. After the Palo Alto attack, as stressed repeatedly in the Amended Complaint, multiple SolarWinds employees recognized or were alerted to the similarity with the previously "unique" attack at USTP. *See* AC ¶¶ 279-287 (repeatedly stressing similarity of the attacks). The timeline of events makes this clear:

July 1, 2020 – Brown determines that USTP is one of two things (1) an attacker already present on USTP system or (2) an attacker looking for ways to utilize Orion in larger attacks. AC ¶ 272.

Oct. 7, 2020 – Palo Alto alerts SolarWinds that Orion BusinessLayer downloaded malicious software; SolarWinds' Information Security Team describes it as a "breach similar to DOJ [USTP]." ECF No. 122-1 at 2-3.

Oct. 14, 2020 – Brown forwards description of similarities between Palo Alto and USTP incidents. ECF No. 122-1 at 2.

Nov. 5, 2020 – According to SolarWinds' call notes, Palo Alto describes the malicious download as occurring during a red team exercise. ECF No. 116-1 at 11.

Nov. 9, 2020 – Palo Alto emails SolarWinds asking them to focus their investigation around two dates, saying, "Our theory is that [SolarWinds] was exploited sometime around 9/28 to stage the subsequent malware download a week later on 10/5." ECF No. 116-1 at 7.

Nov. 24, 2020 – After SolarWinds' asks for a statement from the red team to confirm whether there is an unknown vulnerability at play, Palo Alto responds, "At this point I think we're looking at an unknown vulnerability at play." ECF No. 116-1 at 4.

Nov. 25, 2020 – After SolarWinds asks whether it could speak with the red team, Palo Alto declines and says, "I'd highly encourage you to handle this as though it's an external attacker." ECF No. 116-1 at 3.

All of those facts support the inference that by October 14, given the second incident involving Orion's BusinessLayer, Brown knew, or was reckless or negligent in not knowing, that of his two possible scenarios, it was someone using Orion, and that there were increased risks that should have been disclosed. *See e.g., Meyer v. Jinkosolar Holdings Co., Ltd.*, 761 F.3d 245, 251 (2d Cir. 2014) ("A generic warning of a risk will not suffice when undisclosed facts on the ground would substantially affect a reasonable investor's calculations of probability").

Third, Defendants erroneously argue that their arguments do not present a factual dispute. But as shown by the numerous citations to various documents, the attempts by Defendants to draw different inferences than those asserted in the Amended Complaint, and the arguments about whether an incident occurring during a red team exercise can be described as an attack, there are factual disputes which are only appropriate for resolution after full discovery. The Court need not, and should not, decide this factual question based on an incomplete record of emails and instant message logs as opposed to a full documentary and testimonial record. The Court should therefore disregard Defendants' attempt to transform its motion to dismiss into a motion for summary judgment based upon incomplete and self-serving characterizations of the record.

Respectfully submitted,

/s/ Christopher M. Bruckmann
Christopher M. Bruckmann
John J. Todor
(admitted *pro hac vice*)
Kristen M. Warden
(admitted *pro hac vice*)
William B. Ney
(admitted *pro hac vice*)
Benjamin Brutlag
Lory Stone
(admitted *pro hac vice*)
Christopher J. Carney
Securities and Exchange Commission
100 F Street, NE
Washington, D.C. 20549
202-551-5986 (Bruckmann)
202-551-5381 (Todor)
202-551-4661 (Warden)
202-551-5317 (Ney)
202-551-2421 (Brutlag)
202-551-4931 (Stone)
202-551-2379 (Carney)
BruckmannC@sec.gov
TodorJ@sec.gov
WardenK@sec.gov
NeyW@sec.gov
BrutlagB@sec.gov
StoneL@sec.gov
CarneyC@sec.gov

Attorneys for Plaintiff
Securities and Exchange Commission